Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the subject application.

Listing of Claims:

24. (Currently Amended) A method, comprising:

receiving, by a network adapter, a security association (SA) and a first integrity indicator, said SA and first integrity indicator being generated by an information handling apparatus (IHA) and provided to said network adapter via a network infrastructure;

generating, by said network adapter, a second integrity indicator based on said SA; and

verifying, by said network adapter, that said SA within said network adapter is substantially similar the SA generated by said IHA by comparing said first integrity indicator to said second integrity indicator.

25. (Currently Amended) The method of claim 24, further comprising:

generating, by said IHA, said first integrity indicator based on said SA using a data checking integrity method selected from the group consisting of: checksum, cyclical redundancy checking, Huffman coding, parity checking and ~~has~~ hash computations.

26. (Currently Amended) The method of claim 24, further comprising:

generating, by said network adapter, said second integrity indicator based on said SA using a data checking integrity method selected from the group consisting of: checksum, cyclical redundancy checking, Huffman coding, parity checking and ~~has~~ hash computations.

27. (Previously Presented) The method of claim 24, further comprising:

indicating, by said network adapter, the integrity of said SA to said IHA.

28. (Previously Presented) The method of claim 24, further comprising:

setting an integrity error bit in a memory in the IHA.

29. (Currently Amended) An apparatus, comprising:

a network adapter comprising an integrated circuit, said integrated circuit is capable of receiving a security association (SA) and a first integrity indicator, said SA and first integrity indicator being generated by an information handling apparatus (IHA) and provided to said network adapter via a network infrastructure, said integrated circuit being further capable of generating a second integrity indicator based on said SA, said integrated circuit being further capable of verifying that said SA received by said integrated circuit is substantially similar the SA generated by said IHA by comparing said first integrity indicator to said second integrity indicator.

30. (Currently Amended) The apparatus of claim 29, wherein:

said IHA being capable of generating said first integrity indicator based on said SA using a data checking integrity method selected from the group consisting of: checksum, cyclical redundancy checking, Huffman coding, parity checking and ~~has~~ hash computations.

31. (Currently Amended) The apparatus of claim 29, wherein:

said integrated circuit being further capable of generating said second integrity indicator based on said SA using a data checking integrity method selected from the group consisting of: checksum, cyclical redundancy checking, Huffman coding, parity checking and ~~has~~ hash computations.

32. (Previously Presented) The apparatus of claim 29, wherein:

said integrated circuit being further capable of indicating the integrity of said SA to said IHA.

33. (Previously Presented) The apparatus of claim 29, wherein:

said integrated circuit being further capable of setting an integrity error bit in a memory in the IHA.

34. (Currently Amended) An article comprising:

a storage medium storing instructions that when executed by a machine result in the following operations:

receiving, by a network adapter, a security association (SA) and a first integrity indicator, said SA and first integrity indicator being generated by an information handling apparatus (IHA) and provided to said network adapter via a network infrastructure;

generating, by said network adapter, a second integrity indicator based on said SA; and

verifying, by said network adapter, that said SA within said network adapter is substantially similar the SA generated by said IHA by comparing said first integrity indicator to said second integrity indicator.

35. (Currently Amended) The article of claim 34, wherein said instructions that when executed by said machine result in the following additional operations:

generating, by said IHA, said first integrity indicator based on said SA using a data checking integrity method selected from the group consisting of: checksum, cyclical redundancy checking, Huffman coding, parity checking and ~~has~~ hash computations.

36. (Currently Amended) The article of claim 34, wherein said instructions that when executed by said machine result in the following additional operations:

generating, by said network adapter, said second integrity indicator based on said SA using a data checking integrity method selected from the group consisting of: checksum, cyclical redundancy checking, Huffman coding, parity checking and ~~has~~ hash computations.

37. (Previously Presented) The article of claim 34, wherein said instructions that when executed by said machine result in the following additional operations:

indicating, by said network adapter, the integrity of said SA to said IHA.

38. (Previously Presented) The article of claim 34, wherein said instructions that when executed by said machine result in the following additional operations:

setting an integrity error bit in a memory in the IHA.

39. (Currently Amended) A system, comprising:

at least one network adapter being capable of being coupled to an information handling apparatus (IHA) via a bus, said network adapter comprising an integrated circuit capable of receiving a security association (SA) and a first integrity indicator, said SA and first integrity indicator being generated by said IHA and provided to said network adapter via a network infrastructure, said integrated circuit being further capable of generating a second integrity indicator based on said SA, said integrated circuit being further capable of verifying that said SA received by said integrated circuit is substantially similar the SA generated by said IHA by comparing said first integrity indicator to said second integrity indicator.

40. (Currently Amended) The system of claim 39, wherein:

said IHA being capable of generating said first integrity indicator based on said SA using a data checking integrity method selected from the group consisting of: checksum, cyclical redundancy checking, Huffman coding, parity checking and ~~has~~ hash computations.

41. (Currently Amended) The system of claim 39, wherein:

said integrated circuit being further capable of generating said second integrity indicator based on said SA using a data checking integrity method selected from the group consisting of: checksum, cyclical redundancy checking, Huffman coding, parity checking and ~~has~~ hash computations.

42. (Previously Presented) The system of claim 39, wherein:

said integrated circuit being further capable of indicating the integrity of said SA to said IHA.

43. (Previously Presented) The system of claim 39, wherein:

said integrated circuit being further capable of setting an integrity error bit in a memory in the IHA.